WEB FORENSICS FOR TACKLING TERRORISM INVESTIGATION

TERRORISM AROUND THE WORLD
Terrorism Has Evolved

Major technological advancements have been made over the past decade, affecting nearly every industry and every aspect of day-to-day life. It is no surprise that crimes and terrorism have evolved as well. Today, we see three major forms of terrorism:

1. Conventional or physical terrorism: Operates in the physical world, and involves physical attacks, such as bombs, shootings, and hijackings.

2. Techno-terrorism: Operates in the physical world in order to create cyberspace disruption, such as the use of bombs to destroy information technology infrastructure.

3. Cyberterrorism: Operates exclusively in cyberspace, and typically involves hacking, accessing or exposing sensitive data, taking control of sensitive security systems, and other forms of digital disruption.

Awareness of cyberspace risks and security challenges, including web forensics, has increased among government agencies, especially after the events of 9/11. From cyber risks like viruses used for espionage and malware to attack and control systems, to social media posts and data on the dark web indicating a possible physical attack, the physical and digital realms have collided, and must be used together in the fight against terrorism.

Social Media as a Criminal Platform

Not all attacks are state-level terrorism. A good example of this is the El Paso tragedy that occurred in August 2019. It is believed that online incitement led white supremacists to commit a mass shooting, killing twenty-two people and injuring twenty-four. The incident is treated by the U.S. Department of Justice as domestic terrorism. The suspect’s manifesto was published on 8chan, a platform notoriously used by criminals – specifically mass shooters and white supremacists. This is not a unique scenario; there have been numerous situations involving mass shootings and attacks in which the perpetrators posted their beliefs, and even their detailed plans, before carrying out criminal
actions. In this day and age, terrorist groups are known to use social media to spread their propaganda, communicate with one another, and coordinate their efforts, especially before an attack.

**The Deep and Dark Web**

The internet is a powerful tool for terrorists and criminals, but it is not all open-source and easy to access. National security agencies face constant challenges posed by the deep web and dark web. Unlike the “open” or “surface” web, which is any part of the internet that is accessible by means of regular browsers and indexed by search engines, the deep web features content that cannot be found by common search engines. The dark web is part of the deep web, and requires special browsers in order to access its content, such as Freenet and Tor. The dark web is commonly linked to criminal activity and illegal marketplaces, while the deep web also includes legitimate websites, such as certain social media pages, company intranets, etc. Criminals are constantly taking advantage of these portions of the internet to conduct their nefarious operations with minimal visibility. According to the United Nations Office on Drugs and Crime (UNODC), the internet is used for various terrorist purposes, including:

- Propaganda
- Recruitment
- Incitement
- Radicalization
- Financing
- Training
- Planning and communications
- Execution
- Cyberattacks

According to an article in The Guardian in 2018, “terrorists and extremists are creating a growing number of safe havens on the darknet to plot future attacks, raise funds, and recruit new followers.” Criminals are “hiding in the shadows” of the darknet, and evading security and intelligence agencies by using encrypted messaging services and anonymous cryptocurrencies to generate terror.

According to an article in The Guardian in 2018, “terrorists and extremists are creating a growing number of safe havens on the darknet to plot future attacks, raise funds, and recruit new followers.” Criminals are “hiding in the shadows” of the darknet, and evading security and intelligence agencies by using encrypted messaging services and anonymous cryptocurrencies to generate terror.

Terrorists not only aim to kill but also to divide our societies and spread hatred. That feeling of insecurity that terrorists try to create must be of the greatest concern to us. Increasing polarization and the rise of extremist views is a concern for EU Member States and Europol”, said Catherine De Bolle, Europol’s Executive Director. “I am confident that the efforts of law enforcement, security services, public authorities, private companies, and civil society have substantially contributed to the decrease in terrorist violence in the EU. Terrorism affects real people and that is why we will never stop our efforts to fight terrorism and to prevent victims.
funds. Researchers at the Henry Jackson Society, a foreign policy think tank, said that ISIS encouraged its members to use Telegram, an encrypted communication application. In November 2017, an organization linked with Al Qaida used Telegram to campaign for funding with bitcoin. Additionally, the dark web contains numerous sites with dangerous content, such as instructions on how to create triacetone triperoxide, or TATP, a highly unstable explosive that can be made from household chemicals. TATP was used by jihadists in the Paris attacks in November 2015, as well as in Brussels in March 2016, Manchester in May 2017, and London in September 2017.

**Governments Constantly Invest in Solutions**

Terrorist attacks are carried out with the goal of causing damage and intimidation by using violent means, and terrorists have learned how to use all of the tools available to them in order to reach their goals. As such, governments and law enforcement agencies around the world do everything they can to stay one step ahead of dangerous criminals and protect civilians.

Governments require solutions that combine the physical realm and cyberspace in order to battle terrorism, alongside legislation and military power. Even in cyber attacks, there are often additional physical and personnel elements and methods involved, such as the recruitment of terrorists and terrorist collaborators.

In 2019, the United Kingdom government announced a £36m investment in cyber defense solutions. In the same year, additional efforts were made by the European security organization Europol to advance cybersecurity measures across the continent.

According to Gartner, spending on information security alone will exceed $124 billion worldwide in 2019. According to forecasts by IDC, the U.S. will spend the most on cybersecurity compared to other countries, and at an expected $44.7 billion in 2019, with manufacturing and government accounting for 20% of that. Additionally, governments are constantly investing in open-source intelligence (OSINT) and web intelligence (WEBINT) solutions to help prevent physical and cyber attacks. These solutions are made
for analyzing data in online sources, such as social media and the dark web, to discover suspicious communications and activities.

**Terrorism in Numbers**

Since 2001, terrorist attacks have gone from being relatively low-level to skyrocketing across the world. Image 1 below depicts how terrorism has been playing a larger role in our lives as the years have gone by between 2001 and 2017, not sparing any surface of the globe.

Many of the deadliest attacks are geographically concentrated in conflict-ridden regions, such as the Middle East, Africa, and South Asia, where a staggering 95% of deaths resulting from terrorist attacks occurred in 2017. In these regions, there is an average of 2.4 fatalities per attack in 2016 compared to 1.3 fatalities in non-conflict countries.

Over the past ten years alone, an average of 21,000 people have been killed worldwide each year by terrorists, with the number reaching a high of 44,000 in 2014. In 2017, 0.05% of all global deaths were a result of terrorism – that’s 26,000 people. Public concern is high, and in many countries, over half have said that they were concerned about being a victim of terrorism.

Beyond deadly attacks, there is a shift toward simpler attacks
against non-traditional targets since 2014 - with such unconventional tactics proving to be more effective. In 2019, British Prime Minister Theresa May said that the United Kingdom had foiled 13 Islamist terrorism plots and 4 far-right plots since March 2017, when last year’s attack near the Houses of Parliament occurred. In the European Union more widely, a total of 142 failed, foiled, and completed attacks were reported by eight EU Member States in 2016. Globally, attacks against civilians increased by 17 percent from 2015 to 2016 – targeting private citizens and property.

<table>
<thead>
<tr>
<th>Region</th>
<th>Total Attacks</th>
<th>% of Total</th>
<th>% Change from 2016</th>
<th>Total Deaths</th>
<th>% of Total</th>
<th>% Change from 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle East &amp; North Africa</td>
<td>3780</td>
<td>35%</td>
<td>-38%</td>
<td>10819</td>
<td>41%</td>
<td>-44%</td>
</tr>
<tr>
<td>South Asia</td>
<td>3430</td>
<td>31%</td>
<td>-6%</td>
<td>7664</td>
<td>29%</td>
<td>-2%</td>
</tr>
<tr>
<td>Sub-Saharan Africa</td>
<td>1970</td>
<td>18%</td>
<td>-5%</td>
<td>6712</td>
<td>25%</td>
<td>1%</td>
</tr>
<tr>
<td>Southeast Asia</td>
<td>1020</td>
<td>9%</td>
<td>-5%</td>
<td>811</td>
<td>3%</td>
<td>27%</td>
</tr>
<tr>
<td>Western Europe</td>
<td>291</td>
<td>3%</td>
<td>7%</td>
<td>83</td>
<td>0%</td>
<td>-65%</td>
</tr>
<tr>
<td>South America</td>
<td>172</td>
<td>2%</td>
<td>8%</td>
<td>101</td>
<td>0%</td>
<td>16%</td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>110</td>
<td>1%</td>
<td>-18%</td>
<td>101</td>
<td>0%</td>
<td>-10%</td>
</tr>
<tr>
<td>North America</td>
<td>97</td>
<td>1%</td>
<td>29%</td>
<td>124</td>
<td>0%</td>
<td>70%</td>
</tr>
<tr>
<td>Australias &amp; Oceania</td>
<td>12</td>
<td>0%</td>
<td>20%</td>
<td>4</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Central Asia</td>
<td>7</td>
<td>0%</td>
<td>-59%</td>
<td>6</td>
<td>0%</td>
<td>-71%</td>
</tr>
<tr>
<td>East Asia</td>
<td>7</td>
<td>0%</td>
<td>-13%</td>
<td>16</td>
<td>0%</td>
<td>-50%</td>
</tr>
<tr>
<td>Central America &amp; Caribbean</td>
<td>4</td>
<td>0%</td>
<td>33%</td>
<td>4</td>
<td>0%</td>
<td>-56%</td>
</tr>
<tr>
<td>Worldwide Total</td>
<td>10900</td>
<td>100%</td>
<td>-20%</td>
<td>26445</td>
<td>100%</td>
<td>-24%</td>
</tr>
</tbody>
</table>

Overall, South Asia experienced the most terrorist activity in the last 15 years, while Central and South America were least affected. The MENA region had the sharpest increase in terrorism during that time period. Moreover, since 2002, eight of the nine regions in the world experienced an increase in terrorism, until quite recently in 2016. North America was the only region to experience a reduced impact since 2002. Only starting from 2016 is there a general decrease in terrorist attacks worldwide, as can be seen in Image 2 above.

On the other hand, the number of countries affected by terrorism is growing as we speak. Image 3 below shows a snapshot of the 2019 Global Terrorism Index. Countries most affected are in dark red, with Afghanistan taking the lead, while countries less affected are in light green.

The same information is illustrated below on the heatmap in Image 4, which provides a global overview of the countries and regions most affected by terrorism in 2019.
WEB FORENSIC USES & CHALLENGES

The Use of Web Forensics
Digital or web forensics is a process used by security analysts and investigators, and entails identifying, extracting, analyzing, and documenting digital evidence that can be used in investigations and the court of law. It is a science and an art, as it involves complicated and creative solutions and methods in order to discover critical information from digital sources, like computers, smartphones, servers, networks, and more. Web forensics is an effective tool that helps government agencies in solving complicated cases and preventing crimes that contain digital footprints.

Analysts and investigators use every tool available to them to prevent, mitigate, and deal with attacks and their consequences. They are faced with the challenge of identifying people, properties, and governments that are vulnerable to attacks, and understanding to what extent these vulnerabilities could be exploited, and what the damages could be. Additionally, they are tasked with establishing effective measures to protect these assets, using cybersecurity implementations, as well as WEBINT and OSINT solutions.
Overwhelming Challenges

The data is out there, but it comes with challenges:

Too Much Data

There are vast amounts of data out there; it is an endless pool containing camouflaged information that is needed to stop attacks from harming citizens. Advances in communication technologies, along with internet adoption around the world over the last decade, have created a situation where data travels faster than authorities can respond to it. On the other hand, this also means that authorities have access to more data than ever before, and can harness it to prevent criminals from carrying out their plans. Terrorists use social media and the dark web to communicate and operate, sharing critical information that can be used to stop them. Analysts need to collect, process, prioritize, and take action on the right piece of data. Without knowing exactly where to look at any given time, this is an impossible mission to accomplish.

Siloed Systems

Analysts must gather and analyze data using siloed systems and numerous sources, such as the open web, deep web, dark web, platform and application solutions, and more. This is often done manually, as they piece pertinent information together to create a complete and detailed picture of an incident. Like anything that involves manual work, this leaves them open to human error, and may risk leaving behind undiscovered information that could negatively affect investigations. For agencies, this also increases the use of operational resources significantly, from monetary resources to manpower.
Slow Response Times
When it comes to terror attacks and crimes that place citizens at risk, it is crucial to be able to find, analyze, and react to critical data in real-time. Due to the vast amounts of data involved, discovering helpful information may take too long. While systems with real-time alerts do exist, they often generate unreliable alerts, false positives, or even fail to report suspicious incidents at all. In many cases, these systems hinder the effectiveness of the analysts using them or they are not used at all due to their unreliable results.

Complex Solutions
Web intelligence solutions are usually designed with analysts and technologically-savvy investigators in mind. This is extremely limiting for security agencies, as they want all of their investigators to be able to benefit from data that can be found online pertaining to their cases. In many circumstances, when it comes to privacy protection. Analysts and investigators are constantly faced with the challenge of accessing information and complying with all privacy regulations at the same time. This is not always possible, and can result in important information being inaccessible or overlooked.

Privacy Compliance
The use of online platforms and social media has increased over the past several years, alongside awareness and regulations. Lengthy and complicated training or onboarding is required when adopting new solutions, because they are simply too complex and not intuitive enough.

Missing the Big Picture
Due to the amount of data that needs to be analyzed, it is difficult to take a step back and view multiple pieces of information as a whole. In most cases involving manual analysis, investigators will focus on each piece separately and may not be
able to see how they come together. This “laser” type view often becomes evident only after the fact, when it’s too late to act and prevent an attack from taking place.

Creating Suspect Profiles
Analysts spend long periods of time collecting and analyzing data in order to better understand suspects and create a suspect profile. This requires uncovering basic information such as name, number, and address, as well as an in-depth understanding of the suspect’s character, hobbies, interests, behavior, and social circle. The entire process is extremely time-consuming, which not only demands a high amount of human and other resources, but also delays investigations.

Engaging with Suspects
Once a suspect is identified, criminal investigators will often attempt to engage with them in order to obtain additional crucial information that is relevant to the terrorist case. This can be done by anonymously accessing the web through secured browsing, and then carefully building web profiles (avatars) that can be used as undercover personas to communicate with suspects. In many cases, multiple avatar profiles must be managed simultaneously, which is energy consuming and leaves riskroom for non-compliance with applicable custody policy; particularly, if not performed at the highest levels of excellence.

While there are many challenges, web forensics allows investigators to track down criminals from anywhere in the world, and helps to produce evidence that can stop criminals and prevent their plans from coming to fruition.

Different Types of Solutions
There are many different types of digital forensics, and each type features numerous solutions. Digital forensics has multiple sub-disciplines:

Computer Forensics
The objectives of computer forensics are to identify, recover, analyze, preserve, and report on evidence found on
computers and storage media. This is done in a manner that can help an investigation with relevant information to be presented before a judge.

**Network Forensics**
Network forensics involves monitoring, capturing, storying, and analyzing events and activities on networks. This is done with the goal of discovering the source of various attacks and abnormal behavior that could indicate a threat.

**Mobile Forensics**
Forensics involving mobile devices is critical with today's use of smartphones, PDAs, GPS devices, tablets, game consoles, and more. These devices can contain electronic evidence from a suspect's communication pertaining to a possible crime.

**Digital Image Forensics**
Digital images are analyzed using numerous tools. Authentication tools use metadata from the image to ascertain its history, while more advanced solutions are able to scan the images themselves to search for inconsistencies that may indicate forgery or provide further evidence of a crime. Face recognition tools, used also in video forensics, allow investigators to identify suspects around the world, and on different online platforms, in order to verify their identity and track their activities.

**Digital Video and Audio Forensics**
In addition to face recognition tools, investigators must be able to analyze digital video and audio files to evaluate the authenticity and the files' actual content. This is often used to discover whether a file has been tampered with or altered, especially when it must be used in court or as a lead in an investigation.

**Memory Forensics**
Also called live acquisition, memory forensics is the recovery of evidence from the RAM of a running computer. There are many additional sub-categories that continue to evolve as technology advances. This includes forensics focused on malware, email, databases, wireless networks, and more. In a single investigation, many types of forensics solutions may be used in order to obtain critical information and develop a bigger picture of a possible crime.

While web forensics began outside the mainstream of conventional forensic science, it is now fully recognized as a branch of forensic science. Web forensics continues to expand as technology advances and new types of digital data are created every day.

Despite the challenges of web forensics, governments continue to invest time and resources in scouring the web (open, deep, and dark) for pertinent information. The information is out there – sifting through it is where things get hard, but it doesn’t have to be that way.

Cobwebs Technologies is a world-leading developer of
AI-powered WEBINT solutions used by national security and law enforcement agencies around the globe. With Cobwebs Technologies’ innovative data-driven products and robust technology solutions, government agencies can better identify and respond to threats in real-time, and create safer environments for civilians.

The challenges typically faced by analysts and investigators are easy to overcome with the right technology on their side:

**Never Too Much Data**
Cobwebs Technologies’ platform is powered by artificial intelligence and machine learning algorithms capable of scanning through the web’s endless stream of content. This includes racing through vast amounts of data on various digital channels, such as social media, open web, deep web, dark web, and mobile applications. Cobwebs Technologies allows investigators to automate and streamline their web forensics processes, while gaining in-depth intelligence insights – using fewer resources and a fraction of the time.

**Centralized Platform**
Siloed solutions are a part of the past. It is critical for investigators to have a centralized solution that reduces both wasted resources and human error. Cobwebs Technologies’ platform houses a multitude of features and capabilities in one place, including:

- Image analysis
- Face recognition
- Natural language processing
- Predictive analysis
- Group analysis
- Social network analysis
- Pattern recognition
- Geo-fencing and alerting

By using one centralized platform, investigators can transform single leads into fully developed, end-to-end investigations.
Real-Time Responses
Artificial intelligence and machine learning enable fast aggregation and analysis of data. As a result, government agencies can benefit from a system that continually analyzes real-time information and searches for historical data. Cobwebs Technologies has developed a fully automated platform that generates real-time alerts, while collecting and analyzing data from digital channels at every given moment. Specific inputs can be defined as triggers to automate alerts in order to stay ahead of ongoing incidents and critical information.

Intuitive and User-Friendly
Cobwebs Technologies has developed a simple and user-friendly engine that was designed by top security and technology experts, specifically with analysts and investigators in mind. Every product feature and the entire user experience were developed with the purpose of creating more efficient and easy-to-understand web forensics processes.

Clear Big Picture
With Cobwebs Technologies’ advanced research capabilities, analysts can easily add that missing piece of the puzzle needed to create a clear big picture. Exclusive technology that combines automation, machine learning,
and artificial intelligence allows agencies to analyze and connect the dots to discover hidden leads, and extract intelligence insights from the web’s big data.

Comprehensive Suspect Profiles
The Cobwebs Technologies platform provides automated profiling insights, and allows investigators to discover and extract critical data to create a target profile. This includes malicious activities, social relations and connections, online activities, geographical data for location-based intelligence, social groups and hierarchies, and more. Investigators can search for people and keywords, gain critical operational insights and situational awareness, collect real-time intelligence, and identify new targets, all while uncovering potential profiles and groups across the web.

Suspect Engagement and Avatar Attribution Management
In addition to its many analytics features, the Cobwebs Technologies platform includes a complementary solution that enables avatar attribution management. This allows investigators to anonymously and securely reduce human error and streamline the process of engaging with suspects, streamlining the communication process while greatly reducing the risks of human error and non-compliance with relevant investigation policies.

About Us
Cobwebs Technologies’ platform has been used successfully by leading security agencies around the world, from a European agency that was able to discover an ISIS recruiter to another agency that discovered a terrorist threat and prevented a potential attack in Central America. Led by a team of specialized professionals with military, intelligence, and technology backgrounds, Cobwebs Technologies brings extensive experience and vast knowledge to the table with its innovative and cutting-edge systems.

View a demo of Cobwebs Technologies’ platform to discover the true potential of web intelligence and digital forensics.